LA PROTECCIÓN DE LA INFORMACIÓN EN LA ÉPOCA DEL PHISHING

NOTI 339 – Septiembre de 2023

Algunas de las señales de alerta que indican que un mensaje puede ser un intento de phishing:

- Le solicitan realizar pago, haciendo clic en un enlace para liberar la entrega de un paquete, que ni usted sabe que existe.
- Entidades financieras le informan que su cuenta o su producto ha sido bloqueado y requiere confirmar su identidad a través de un link.
- Plataformas de correo que le indican que su cuenta ha sido bloqueda y debe ingresar a un link para validar su identidad.

Imagen tomada de: https://share.america.gov/es/como-proteger-su-telefono-inteligente-de-ataques-cibernetico s/

Con el auge de los teléfonos inteligentes y el uso que les damos en nuestro diario vivir, tenemos un caldo de cultivo para que los amigos de lo ajeno, en materia informática, estén al acecho. Estos dispositivos móviles los llevamos a todas partes con nosotros y se convirtieron en el epicentro de nuestras vidas; son los aparatos con los que realizamos nuestros movimientos bancarios, revisamos nuestro correo electrónico personal y corporativo; tomamos fotos, utilizamos tanto los servicios de Google que hasta conoce nuestras búsquedas en Internet, los sitios que hemos visitado (tanto físicos como virtuales); y toda esta información resulta altamente valiosa para quienes puedan acceder a ella y mejor aún, para quienes la conozcan y la puedan utilizar.

Indudablemente vivimos una época de gran peligro para la confidencialidad de nuestra información; generando así la necesidad de conocer las amenazas que nos rodean, con el fin de estar preparados para enfrentarlas.

Algunas veces hemos podido escuchar la palabra Phishing, esta se refiere a la forma en que los delincuentes tratan de obtener información personal de sus víctimas a través de medios de engaño que, usualmente, involucran los diferentes canales por los que nos comunicamos, bien sea por correo electrónico, llamadas telefónicas, mensajería instantánea (WhatsApp, Telegram, etc.), mensajes de texto, redes sociales, entre otros muchos. Estos son los canales preferidos por los ciberdelincuentes para hacer que caigamos en sus trampas.

Imagen de: https://centronet.com.co/que-es-y-como-afecta-el-phishing-la-seguridad-digital/

Algunas veces hemos podido escuchar la palabra Phishing, esta se refiere a la forma en que los delincuentes tratan de obtener información personal de sus víctimas a través de medios de engaño que, usualmente, involucran los diferentes canales por los que nos comunicamos, bien sea por correo electrónico, llamadas telefónicas, mensajería instantánea (WhatsApp, Telegram, etc.), mensajes de texto, redes sociales, entre otros muchos. Estos son los canales preferidos por los ciberdelincuentes para hacer que caigamos en sus trampas.

Algunas de las modalidades que están muy de moda en nuestro país implican mensajes de texto, correo electrónico o mensajes a través de la plataforma WhatsApp, entre los cuales enumeramos algunos que se presentan en nuestro medio:

- Mensajes que aparentan ser de la empresa 4/72 de envíos nacionales pidiendo pagar por un envío o un domicilio que se tiene pendiente.

- Nos pueden llegar mensajes de diferentes entidades financieras anunciando que los datos de seguridad de la cuenta han sido cambiados o que nos han bloqueado por seguridad nuestras tarjetas de crédito y que debemos confirmar nuestra identidad.

- Saludos en WhatsApp desde números de contacto con códigos indicativos internacionales de países exóticos como Corea del Norte (+242), Hong Kong (+852), Filipinas (+62), entre otros.

- Correos electrónicos indicando que nuestras cuentas de diferentes servicios han sido bloqueadas, estos servicios incluyen correos como los de Google, Outlook, Amazon, entre otras.

Lo particular de todos estos casos es que en la mayoría de ellos se proveen enlaces en los cuales se debe dirigir la víctima del phishing para poder realizar la acción solicitada en el mensaje; sin embargo, estos links que nos proveen nos llevaran a sitios falsos diseñados específicamente para capturar nuestros datos sensibles y poder hacer luego uso de dicha información para cometer actos que nos pongan en riesgo de tener pérdidas bancarias o para estafar a otras personas, en nombre nuestro.

La utilización de antivirus, realizar actualizaciones, no dejarnos presionar para entregar información personal para evitar supuestas suspensiones de servicios o sanciones monetarias, ayudan a reducir la posibilidad de ser víctimas de phishing.

Imagen tomada de:
https://computerworldmexico.com.mx/como-puedes-ayudar-a-proteger-tu-organizacion-de-los-ataques/

Por: Santiago Duque Giraldo, Coordinador
Área de Conocimiento y Desarrollo
ASR S.A.S.

Medellín, Colombia
+573103923352 - 3233453366
asr@asr.com.co
http://www.asr.com.co/

Una manera rápida de identificar estos mensajes maliciosos pasa por los errores en redacción y ortografía que pueden resultar evidentes; así mismo, podemos identificar en muchas ocasiones que el link que se menciona, no direcciona al sitio web verdadero de la entidad que tratan de suplantar; de todas maneras, no sugerimos en ningún caso acceder a los links que se relacionan dado que estos pueden descargar programas maliciosos sólo con la acción de abrirlos.

Para podernos proteger de estos males tecnológicos, serán útiles algunas recomendaciones de protección, entre las que se incluye mantener nuestros equipos actualizados siempre con las últimas versiones de los programas, mantener un antivirus siempre activo, tener activos los filtros anti spam en los servicios de telefonía, mensajería de texto y correo en nuestros dispositivos móviles y el computador de escritorio, descargar aplicaciones de las tiendas oficiales y no desde links en sitios desconocidos; y, ante todo, tener la malicia de poder identificar estos trucos en el instante en que se nos presenten en nuestro día a día.

asr@asr.com.co